

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Toru TERAUCHI

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: METHOD FOR ENCRYPTING CONTENT, AND METHOD AND APPARATUS FOR DECRYPTING
ENCRYPTED DATA

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e): Application No. Date Filed
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:


<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2002-305970	October 21, 2002

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- ☐ (B) Application Serial No.(s)
- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.


Marvin J. Spivak

Registration No. 24,913

Customer Number

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

C. Irvin McClelland
Registration Number 21,124

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年10月21日

出 願 番 号

Application Number:

特願2002-305970

[ST.10/C]:

[JP2002-305970]

出 願 人

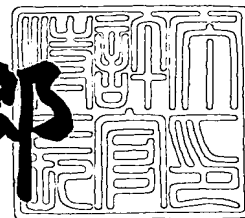
Applicant(s):

株式会社東芝

2003年 3月14日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3016615

【書類名】 特許願

【整理番号】 A000200284

【提出日】 平成14年10月21日

【あて先】 特許庁長官 殿

【国際特許分類】 G09C 1/00

【発明の名称】 コンテンツの暗号化方法及び暗号化されたデータを復号化する復号化方法並びにその装置

【請求項の数】 24

【発明者】

 【住所又は居所】 東京都青梅市末広町2丁目9番地 株式会社東芝青梅工場内

 【氏名】 寺内 亨

【特許出願人】

 【識別番号】 000003078

 【氏名又は名称】 株式会社 東芝

【代理人】

 【識別番号】 100058479

 【弁理士】

 【氏名又は名称】 鈴江 武彦

 【電話番号】 03-3502-3181

【選任した代理人】

 【識別番号】 100084618

 【弁理士】

 【氏名又は名称】 村松 貞男

【選任した代理人】

 【識別番号】 100068814

 【弁理士】

 【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 コンテンツの暗号化方法及び暗号化されたデータを復号化する復号化方法並びにその装置

【特許請求の範囲】

【請求項 1】

コンテンツ毎にユニークに決まるタイトルキーと端末側から取得された項目情報を含みコンテンツの再生対象を限定する再生対象固有情報とが組み合わされた運用規則情報と、

前記タイトルキーと前記再生対象固有情報とから生成される暗号化キー情報を基に暗号化されている暗号化コンテンツ・データとを受け取り、

前記運用規則情報から端末側で取得可能な項目情報を基に暗号化コンテンツ・データの再生可能性を判定し、この判定に従って、前記項目情報及びタイトルキーから復号化キーを生成する復号化キー生成部と、

前記コンテンツ・データを前記復号化キー情報を基に復号化する復号化部と、
を具備する暗号化されたデータを復号化する端末装置。

【請求項 2】

前記再生対象固有情報は、再生対象のコンテンツに関する制限項目、前記端末装置を限定する限定項目及びユーザに固有の項目のいずれかの項目を含むことを特徴とする請求項 1 の端末装置。

【請求項 3】

前記暗号化キー情報は、前記再生対象固有情報に依存しない運用規則情報である旨を示すフラグを含むことを特徴とする請求項 1 の端末装置。

【請求項 4】

コンテンツ毎にユニークに決まるタイトルキーと端末側から取得された項目情報を含みコンテンツの再生対象を限定する再生対象固有情報とを基に暗号化したキーワード情報とが組み合わされた運用規則情報と、

前記タイトルキーと前記再生対象固有情報から生成される暗号化キー情報を基に暗号化されている暗号化コンテンツ・データとを受け取り、

前記運用規則情報に含まれる暗号化されたキーワード情報から端末で取得可能

な項目情報を基に暗号化コンテンツ・データの再生可能性を判定し、この判定に従って、前記項目情報及びタイトルキーから復号化キーを生成する復号化キー生成部と、

前記コンテンツ・データを前記復号化キー情報を基に復号化する復号化部と、
を具備する暗号化されたデータを復号化する端末装置。

【請求項 5】

前記再生対象固有情報は、再生対象のコンテンツに関する制限項目、前記端末装置を限定する限定項目及びユーザに固有の項目のいずれかの項目を含むことを特徴とする請求項 4 の端末装置。

【請求項 6】

前記暗号化キー情報は、前記再生対象固有情報に依存しない運用規則情報である旨を示すフラグを含むことを特徴とする請求項 4 の端末装置。

【請求項 7】

コンテンツ毎にユニークに決まるタイトルキー及び端末側から項目情報を取得してコンテンツの再生対象を限定する再生対象固有情報を生成する第 1 の生成部と、

前記タイトルキー及び再生対象固有情報に基づいて暗号化キー情報を生成する第 2 の生成部と、

コンテンツ・データを暗号化キー情報で暗号化する暗号化部と、

前記タイトルキー及び再生対象固有情報から運用規則情報を生成する運用規則生成部と、

を具備するコンテンツの暗号化装置。

【請求項 8】

前記再生対象固有情報は、再生対象のコンテンツに関する制限項目、前記端末装置を限定する限定項目及びユーザに固有の項目のいずれかの項目を含むことを特徴とする請求項 7 の暗号化装置。

【請求項 9】

前記再生対象固有情報に依存しない運用規則情報である旨を示すフラグが運用規則生成部で生成されることを特徴とする請求項 7 の暗号化装置。

【請求項 1 0】

コンテンツ毎にユニークに決まるタイトルキー及び端末側から項目情報を取得してコンテンツの再生対象を限定する再生対象固有情報を生成する第 1 の生成部と、

前記タイトルキー及び再生対象固有情報に基づいて暗号化キー情報を生成し、また、前記再生対象固有情報を基にキーワードを暗号化した暗号化キーワード情報を生成する第 2 の生成部と、

コンテンツ・データを暗号化キー情報で暗号化する暗号化部と、

前記タイトルキー及び暗号化キーワード情報から運用規則情報を生成する運用規則生成部と、

を具備するコンテンツの暗号化装置。

【請求項 1 1】

前記再生対象固有情報は、再生対象のコンテンツに関する制限項目、前記端末装置を限定する限定項目及びユーザに固有の項目のいずれかの項目を含むことを特徴とする請求項 1 0 の暗号化装置。

【請求項 1 2】

前記再生対象固有情報に依存しない運用規則情報である旨を示すフラグが運用規則生成部で生成されることを特徴とする請求項 1 1 の暗号化装置。

【請求項 1 3】

コンテンツ毎にユニークに決まるタイトルキーと端末側から取得された項目情報を含み、コンテンツの再生対象を限定する再生対象固有情報とが組み合わされた運用規則情報と、

前記タイトルキーと前記再生対象固有情報から生成される暗号化キー情報を基に暗号化されている暗号化コンテンツ・データとを受け取る工程と、

前記運用規則情報から端末側で取得可能な項目情報を基に暗号化コンテンツ・データの再生可能性を判定し、この判定に従って、前記項目情報及びタイトルキーから復号化キーを生成する復号化キー生成工程と、

前記コンテンツ・データを前記復号化キー情報を基に復号化する復号化工程と

を具備する暗号化されたデータを復号化する方法。

【請求項 1 4】

前記再生対象固有情報は、再生対象のコンテンツに関する制限項目、前記端末装置を限定する限定項目及びユーザに固有の項目のいずれかの項目を含むことを特徴とする請求項 1 3 の方法。

【請求項 1 5】

前記運用規則情報は、前記再生対象固有情報に依存しない運用規則情報である旨を示すフラグを含むことを特徴とする請求項 1 3 の方法。

【請求項 1 6】

コンテンツ毎にユニークに決まるタイトルキーと端末側から取得された項目情報を含みコンテンツの再生対象を限定する再生対象固有情報とを基に暗号化したキーワード情報とが組み合わされた運用規則情報と、

前記タイトルキーと、前記再生対象固有情報から生成される暗号化キー情報を基に暗号化されている暗号化コンテンツ・データとを受け取る工程と、

前記運用規則情報に含まれる暗号化されたキーワード情報から端末側で取得可能な項目情報を基に暗号化コンテンツ・データの再生可能性を判定し、この判定に従って、前記項目情報及びタイトルキーから復号化キーを生成する復号化キー生成工程と、

前記コンテンツ・データを前記復号化キー情報を基に復号化する復号化工程と

を具備する暗号化されたデータを復号化する方法。

【請求項 1 7】

前記再生対象固有情報は、再生対象のコンテンツに関する制限項目、前記端末装置を限定する限定項目及びユーザに固有の項目のいずれかの項目を含むことを特徴とする請求項 1 6 の方法。

【請求項 1 8】

前記運用規則情報は、前記再生対象固有情報に依存しない運用規則情報である旨を示すフラグを含むことを特徴とする請求項 1 6 の方法。

【請求項 1 9】

コンテンツ毎にユニークに決まるタイトルキー及び端末側から項目情報を取得してコンテンツの再生対象を限定する再生対象固有情報を生成する第 1 の工程と、

前記タイトルキー及び再生対象固有情報に基づいて暗号化キー情報を生成する第 2 の生成工程と、

コンテンツ・データを暗号化キー情報で暗号化する暗号化工程と、

前記タイトルキー及び再生対象固有情報から運用規則情報を生成する運用規則情報生成工程と、

を具備するコンテンツの暗号化方法。

【請求項 2 0】

前記再生対象固有情報は、再生対象のコンテンツに関する制限項目、前記端末装置を限定する限定項目及びユーザに固有の項目のいずれかの項目を含むことを特徴とする請求項 1 9 の暗号化方法。

【請求項 2 1】

前記再生対象固有情報に依存しない運用規則情報である旨を示すフラグが運用規則生成工程で生成されることを特徴とする請求項 1 9 の暗号化方法。

【請求項 2 2】

コンテンツ毎にユニークに決まるタイトルキー及び端末側から項目情報を取得してコンテンツの再生対象を限定する再生対象固有情報を生成する第 1 の生成工程と、

前記タイトルキー及び再生対象固有情報に基づいて暗号化キー情報を生成し、また、前記再生対象固有情報を基にキーワードを暗号化した暗号化キーワード情報を生成する第 2 の生成工程と、

コンテンツ・データを暗号化キー情報で暗号化する暗号化工程と、

前記タイトルキー及び暗号化キーワード情報から運用規則情報を生成する運用規則情報生成工程と、

を具備するコンテンツの暗号化方法。

【請求項 2 3】

前記再生対象固有情報は、再生対象のコンテンツに関する制限項目、前記端

末装置を限定する限定項目及びユーザに固有の項目のいずれかの項目を含むことを特徴とする請求項 2 2 の暗号化方法。

【請求項 2 4】

前記再生対象固有情報に依存しない運用規則情報である旨を示すフラグが運用規則生成工程で生成されることを特徴とする請求項 2 2 の暗号化方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

この発明は、コンテンツ・データを暗号化する暗号化方法及び暗号化されたデータを復号化する方法に係り、特に、音楽や映像の配信サービスにおける著作権保護方式にて利用される暗号化・復号化方法に関する。

【0 0 0 2】

【従来の技術】

近年、インターネット、或いは、携帯電話サービスの普及に伴い、音楽、或いは、映像コンテンツの配信サービスが普及し始めている。このようなサービスにおいては、配信するコンテンツの違法コピーを防ぐために、著作権保護の仕組みが組み込まれている。

【0 0 0 3】

著作権保護方式では、一般的に、あるキー情報を元にコンテンツを暗号化した上で配信し、正規ユーザは、正しいキー情報を受け取った上でこのキー情報を元にコンテンツを復号化し、再生している。暗号化されたコンテンツを不正にコピーした場合には、正しいキー情報を受け取れなくすることにより、コンテンツを正しく復号化できなくして、結果として不正に再生することを防止している。

【0 0 0 4】

通常のサービスでは、こうしたキー情報の他に、運用規則情報と呼ばれる付加的な情報をやりとりすることで、配信したコンテンツのコピー条件や再生条件などを制限することができる。例えば、再生回数を制限したい場合には、再生可能な回数をあらかじめ設定しておき、運用規則情報として組み込んでいる。コンテンツを配信する際には、暗号化されたコンテンツとペアで、キー情報及び運用規

則情報を配信している。配信先では、受け取ったキー情報を元にコンテンツを復号化し、再生準備をするとともに、同時に、運用規則情報を解析し、再生可能回数を調べている。再生可能回数が1以上であれば、再生処理を実行するとともに、同時に、再生可能回数を1減じた後、その値を運用規則情報に反映している。再生可能回数が0であれば、再生処理を中止している。このように、予め指定された回数だけしか再生できないコンテンツを配信することが可能となる。

【0005】

こうしたキー情報、或いは、運用規則情報は、コンテンツ配信サービスにおいては、重要な情報であるため、別途セキュリティを考慮した方式で配信される。例えば、インターネットなどの場合、SSL (Secure Sockets Layer) と呼ばれる方式を用いて、運用規則情報が暗号化されて送受信される。

【0006】

通常、キー情報は、コンテンツ毎にユニークとなるよう、乱数発生器などを用いて生成されたタイトルキーと呼ばれる情報が用いられる。また、タイトルキーと他の情報を組み合わせることで、コンテンツの再生を特定の端末などに限定することができる。例えば、配信元では、再生対象となる端末の製造番号を入手し、タイトルキーと組み合わせることでキー情報を生成し、キー情報を用いてコンテンツを暗号化している。配信元は、配信先へタイトルキー及び暗号化コンテンツを配信している。配信先でコンテンツを再生する際には、再生端末に付けられている製造番号と、タイトルキーとが組み合わせられてキー情報が生成され、キー情報を用いてコンテンツを復号化した上、コンテンツの再生処理がなされる。このとき、再生端末が配信側で予定している端末でない場合には、予定していない端末に付けられた製造番号及びタイトルキーの組み合わせで生成されるキー情報が不正なものとなるため、コンテンツを正しく復号化することができない。

【0007】

このように、タイトルキー及び限定対象となる固有情報が組み合わせられることで、コンテンツの再生できる対象を限定することが可能となる。限定対象としては、再生する端末を限定する場合、再生する個人を限定する場合、蓄積する媒体を限定する場合、あるいはそれらを組み合わせる場合など、様々な場合が想定さ

れる。

【 0 0 0 8 】

【発明が解決しようとする課題】

しかしながら、上記した従来技術においては、コンテンツの再生対象を限定した場合、コンテンツの再生条件を満たしているかどうかは、コンテンツを復号化するまで判断ができない問題がある。また、コンテンツの種類によっては、例えば、PCM (Pulse Code Modulation) 生データのようにデータの中身を見ただけでは正しいかどうか判断ができないようなフォーマットの場合、復号化した結果が正しいかどうか判断できない問題がある。

【 0 0 0 9 】

この発明は、上記の問題を解決するためになされたものであり、その目的は、コンテンツの再生対象を限定した場合においても、コンテンツを再生する際に、再生条件を満たしているかどうかを、コンテンツを復号化しなくても確実に判断できる暗号化方法及び暗号化されたコンテンツを復号化する復号化方法を提供するにある。

【 0 0 1 0 】

【課題を解決するための手段】

この発明によれば、

コンテンツ毎にユニークに決まるタイトルキーと端末側から取得された項目情報を含みコンテンツの再生対象を限定する再生対象固有情報とが組み合わされた運用規則情報と、

前記タイトルキーと前記再生対象固有情報とから生成される暗号化キー情報を基に暗号化されている暗号化コンテンツ・データとを受け取り、

前記運用規則情報から端末側で取得可能な項目情報を基に暗号化コンテンツ・データの再生可能性を判定し、この判定に従って、前記項目情報及びタイトルキーから復号化キーを生成する復号化キー生成部と、

前記コンテンツ・データを前記復号化キー情報を基に復号化する復号化部と、を具備する暗号化されたデータを復号化する端末装置が提供される。

【 0 0 1 1 】

また、この発明によれば、

コンテンツ毎にユニークに決まるタイトルキーと端末側から取得された項目情報を含みコンテンツの再生対象を限定する再生対象固有情報とを基に暗号化したキーワード情報とが組み合わされた運用規則情報と、

前記タイトルキーと前記再生対象固有情報から生成される暗号化キー情報を基に暗号化されている暗号化コンテンツ・データとを受け取り、

前記運用規則情報に含まれる暗号化されたキーワード情報から端末で取得可能な項目情報を基に暗号化コンテンツ・データの再生可能性を判定し、この判定に従って、前記項目情報及びタイトルキーから復号化キーを生成する復号化キー生成部と、

前記コンテンツ・データを前記復号化キー情報を基に復号化する復号化部と、
を具備する暗号化されたデータを復号化する端末装置が提供される。

【 0 0 1 2 】

この発明によれば、また、

コンテンツ毎にユニークに決まるタイトルキー及び端末側から項目情報を取得してコンテンツの再生対象を限定する再生対象固有情報を生成する第 1 の生成部と、

前記タイトルキー及び再生対象固有情報に基づいて暗号化キー情報を生成する第 2 の生成部と、

コンテンツ・データを暗号化キー情報で暗号化する暗号化部と、

前記タイトルキー及び再生対象固有情報から運用規則情報を生成する運用規則生成部と、

を具備するコンテンツの暗号化装置が提供される。

【 0 0 1 3 】

更に、この発明によれば、

コンテンツ毎にユニークに決まるタイトルキー及び端末側から項目情報を取得してコンテンツの再生対象を限定する再生対象固有情報を生成する第 1 の生成部と、

前記タイトルキー及び再生対象固有情報に基づいて暗号化キー情報を生成し、

また、前記再生対象固有情報を基にキーワードを暗号化した暗号化キーワード情報を生成する第2の生成部と、

コンテンツ・データを暗号化キー情報で暗号化する暗号化部と、

前記タイトルキー及び暗号化キーワード情報から運用規則情報を生成する運用規則生成部と、

を具備するコンテンツの暗号化装置が提供される。

【0014】

また、更にこの発明によれば、

コンテンツ毎にユニークに決まるタイトルキーと端末側から取得された項目情報を含み、コンテンツの再生対象を限定する再生対象固有情報とが組み合わされた運用規則情報と、

前記タイトルキーと前記再生対象固有情報から生成される暗号化キー情報を基に暗号化されている暗号化コンテンツ・データとを受け取る工程と、

前記運用規則情報から端末側で取得可能な項目情報を基に暗号化コンテンツ・データの再生可能性を判定し、この判定に従って、前記項目情報及びタイトルキーから復号化キーを生成する復号化キー生成工程と、

前記コンテンツ・データを前記復号化キー情報を基に復号化する復号化工程と

を具備する暗号化されたデータを復号化する方法が提供される。

【0015】

更にまた、この発明によれば、

コンテンツ毎にユニークに決まるタイトルキーと端末側から取得された項目情報を含みコンテンツの再生対象を限定する再生対象固有情報とを基に暗号化したキーワード情報とが組み合わされた運用規則情報と、

前記タイトルキーと、前記再生対象固有情報から生成される暗号化キー情報を基に暗号化されている暗号化コンテンツ・データとを受け取る工程と、

前記運用規則情報に含まれる暗号化されたキーワード情報から端末側で取得可能な項目情報を基に暗号化コンテンツ・データの再生可能性を判定し、この判定に従って、前記項目情報及びタイトルキーから復号化キーを生成する復号化キー

生成工程と、

前記コンテンツ・データを前記復号化キー情報を基に復号化する復号化工程と

を具備する暗号化されたデータを復号化する方法が提供される。

【 0 0 1 6 】

また、更に、この発明によれば、

コンテンツ毎にユニークに決まるタイトルキー及び端末側から項目情報を取得してコンテンツの再生対象を限定する再生対象固有情報を生成する第 1 の工程と、

前記タイトルキー及び再生対象固有情報に基づいて暗号化キー情報を生成する第 2 の生成工程と、

コンテンツ・データを暗号化キー情報で暗号化する暗号化工程と、

前記タイトルキー及び再生対象固有情報から運用規則情報を生成する運用規則情報生成工程と、

を具備するコンテンツの暗号化方法が提供される。

【 0 0 1 7 】

【発明の実施の形態】

以下、図面を参照しながらこの発明の実施例に係るコンテンツの暗号化方法及び暗号化されたコンテンツを復号化する復号化方法について説明する。

【 0 0 1 8 】

図 1 は、この発明の一実施例に係る暗号化処理の為の回路構成を機能ブロックで示すコンテンツ暗号化処理回路である。図 1 に示される回路においては、コンテンツ・データが暗号化部 1 1 0 に入力されて暗号化されて暗号化コンテンツ・ファイルとして出力される。ここで、コンテンツ・データは、暗号化部 1 1 0 において、暗号化キー生成部 1 1 4 で生成される暗号化キーに基づいて暗号化される。この暗号化キーは、コンテンツのタイトル毎に定まるタイトルキー及び再生対象固有情報に基づいて暗号化キー生成部 1 1 4 で生成される。タイトルキーは、タイトルキー生成部 1 1 6 でタイトル毎に生成される。再生対象固有情報は、コンテンツの配布条件に相当する再生対象条件を設定する再生対象条件設定部 1

20からの再生対象条件、コンテンツを再生する機器を限定する端末限定項目情報設定部122からの端末限定項目情報及び個人に固有の情報に基づいてコンテンツの再生を限定する個人固有項目情報設定部124からの個人固有項目情報が再生対象固有情報生成部118に与えられて生成される。再生対象条件設定部120、端末限定項目情報設定部122及び個人固有項目情報設定部124は、再生対象制限項目情報、端末情報及び個人固有項目情報が入出力部（図示せず）を介して供給されるメモリ上の領域が相当し、再生対象固有情報生成部118に与えられる情報は、これらの情報に限定されず、他の情報に代えられても、或いは、他の情報が追加されても良い。

【0019】

タイトルキー生成部116で生成されるタイトルキー及び再生対象固有情報生成部118で生成される再生対象固有情報は、運用規則情報生成部112に与えられて運用規則情報としてファイル化され、この運用規則情報ファイルが出力される。

【0020】

図2は、図1に示されたコンテンツ暗号化処理回路からの暗号化された暗号化コンテンツ・ファイル进行处理する端末の回路構成を機能ブロックで示している。暗号化コンテンツ・ファイル及び運用規則情報ファイルは、ネット網等の通信網を介して送られ、端末の入出力部（図示せず）を介して分離部142に与えられる。受信した暗号化コンテンツ・ファイルは、暗号化コンテンツ・データ記憶部146に格納され、受信した運用規則情報ファイルは、運用情報記憶部144に格納される。これら記憶部は、通常、メモリ上の領域に相当している。図2に示される復号化キー生成部148には、端末の固有情報が供給され、また、端末上で入力された個人情報も供給され、復号化キー生成部148は、これら端末固有情報及び個人情報並びに運用情報から復号化キーを後に説明するように生成している。復号化部150では、暗号化キー生成部148で生成された復号化キーを用いて暗号化コンテンツデータを復号化して図示しない変換部で音声信号及び映像信号に変換されて音声・映像コンテンツとして再生される。

【0021】

次に図 1 及び図 2 に示したコンテンツ暗号化処理回路及び端末回路での処理について図 3 から図 5 を参照して説明する。

【 0 0 2 2 】

図 3 は、この発明の一実施例に係る暗号化処理の手順を示すフローチャートである。コンテンツが暗号化される際には、ステップ S 1 1 に示すように、始めにコンテンツ毎にユニークに決まる固定長のデータがタイトルキーとしてタイトルキー生成部 1 1 6 において生成される。例えば、乱数発生器を用いて 6 4 b i t の乱数データが生成され、タイトルキーに定められる。次に、ステップ S 1 2 に示すように、コンテンツの再生対象を制限するかどうか、また、制限する場合にはどのような組み合わせで制限するかのような再生対象条件が再生対象条件設定部 1 2 0 において設定される。この再生対象条件は、コンテンツ毎にコンテンツの配布元（コンテンツ・プロバイダ）により任意に決められる。次に、ステップ S 1 3 に示すように設定された再生対象条件が端末に限定されるかどうか判定され、端末に限定する場合には、ステップ S 1 4 に示すように対象となる端末の固有情報が端末限定項目情報設定部 1 2 2 で入手される。端末の固有情報としては、例えば、端末の製造番号等があり、端末毎にユニークに決まる情報が固有情報として利用される。ステップ S 1 5 に示すように入手した端末の固有情報は、再生対象固有情報として設定される。

【 0 0 2 3 】

ステップ S 1 3 において、設定された再生対象条件が端末に限定されない場合には、同様に、ステップ S 1 6 において、設定された再生対象条件が個人に限定されるかどうか判定される。個人に限定される場合には、ステップ S 1 7 に示すように、対象となる個人の固有情報が個人固有項目情報設定部 1 2 4 で入手される。この個人情報としては、例えば、クレジットカード番号等があり、個人毎にユニークに決まる情報が固有情報として利用される。入手した個人の固有情報は、ステップ S 1 8 において、再生対象固有情報として設定される。

【 0 0 2 4 】

ステップ S 1 6 において、設定された再生対象条件が個人に限定されない場合には、ステップ S 1 9 に示すように、設定された再生対象条件が端末と個人の組

み合わせに限定されるかどうか判定される。端末と個人の組み合わせに限定する場合には、ステップ S 2 0 及び S 2 1 に示すように対象となる端末の固有情報が入手されると共に個人の固有情報が入手される。入手した端末の固有情報及び個人の固有情報を基にしてステップ S 2 2 に示すように再生対象固有情報が再生対象固有情報生成部 1 1 8 において生成される。この再生対象固有情報としては、例えば、端末固有情報及び個人固有項目情報を X O R 演算処理した演算結果があり、この演算結果が再生対象固有情報に定められる。

【 0 0 2 5 】

ステップ S 1 3、ステップ S 1 6 及びステップ S 1 9 のいずれかにおいて、再生対象条件を限定する場合には、ステップ S 2 3 に示すようにタイトルキー及び再生対象固有情報から暗号化キーが暗号化キー生成部 1 1 4 において生成される。この暗号化キーとしては、例えば、タイトルキー及び再生対象固有情報を X O R 演算処理した演算結果があり、この演算結果が暗号化キーに定められる。

【 0 0 2 6 】

ステップ S 1 9 において、設定された再生対象条件が端末と個人の組み合わせに限定されない場合には、ステップ S 2 4 に示されるように設定された再生対象条件が限定なしかどうか判定され、再生対象が限定されない場合には、ステップ S 2 5 において、タイトルキーがそのまま暗号化キーとして設定される。

【 0 0 2 7 】

ステップ S 2 4 において、設定された再生対象条件が、上記以外の場合には、ステップ S 2 6 に示すように判定処理エラーとしてエラー処理がなされ、処理が終了する。

【 0 0 2 8 】

ステップ S 2 3 において、暗号化キーが設定されると、ステップ S 2 7 に示すように暗号化部 1 1 0 にコンテンツが読み込まれてステップ S 2 8 に示すように暗号化キーを用いてコンテンツが暗号化処理される。その後、ステップ S 2 9 に示すように、暗号化されたコンテンツがファイルに書き出される。ステップ S 3 0 に示すように再生対象固有情報及びタイトルキーが運用規則情報としてファイルに書き出される。

【 0 0 2 9 】

図 4 には、暗号化処理で生成される運用規則情報のデータ構造が示されている。運用規則情報は、再生対象条件を限定するかどうかを示すフラグ 2 0 1 と、再生対象固有情報 2 0 2 及びタイトルキー 2 0 3 から構成される。再生対象を限定する場合には、再生対象限定フラグに 1 が設定され、このフラグ「1」によって、再生対象固有情報が有効であることが示される。逆に、再生対象を限定しない場合には、再生対象限定フラグに 0 が設定され、このフラグ「0」によって、再生対象固有情報が不定となる。暗号化処理で生成された暗号化データと運用規則情報は、サービスに応じてあらかじめ決められた方法で、再生端末へ配信される。

【 0 0 3 0 】

再生端末では、図 5 に示すような手順に従い暗号化されたコンテンツが復号化処理される。

【 0 0 3 1 】

再生端末では、暗号化コンテンツ・ファイルと運用規則情報ファイルがファイル受信部 1 4 2 に入力され、夫々運用規則情報記憶部 1 4 4 及び暗号化コンテンツ・データ記憶部 1 4 6 に記憶される。復号化キー生成部 1 4 8 では、始めにステップ S 3 1 に示されるように配信された運用規則情報が読み込まれる。次に、ステップ S 3 2 において、読み込んだ運用規則情報から再生対象限定フラグが抽出され、再生対象限定フラグが 1 に設定されているかが判断される。フラグに 1 が設定されている場合には、再生対象が限定されていると判断される。従って、ステップ S 3 3 に示すように端末固有情報が再生端末から復号化キー生成部 1 4 8 に入力される。また、ステップ S 3 4 に示すように個人固有項目情報が復号化キー生成部 1 4 8 に入力される。

【 0 0 3 2 】

次に、読み込んだ運用規則情報から再生対象固有情報が抽出され、ステップ S 3 5 に示すように再生対象固有情報が端末固有情報と一致するかが判定される。両者が一致しない場合には、ステップ S 3 6 に示すように同様にして再生対象固有情報が個人固有項目情報と一致するかが判定される。再生対象固有情報が個人

固有項目情報に一致しない場合には、ステップ S 3 7 において、端末固有情報及び個人固有項目情報から固有情報が復号化キー生成部 1 4 8 で生成される。例えば、既に述べたように端末固有情報及び個人固有項目情報が X O R 演算処理され、その演算結果が固有情報として求められる。次に、ステップ S 3 8 において、再生対象固有情報と生成した固有情報が一致するかが判定される。ステップ S 3 5、S 3 6、S 3 7 のいずれかにおいて、運用規則情報内の再生対象固有情報と、上記いずれかの条件が一致される場合には、再生対象であると判断され、ステップ S 3 9 において、運用規則情報内のタイトルキー及び再生対象固有情報から復号化キーが復号化キー生成部 1 4 8 で生成される。例えば、タイトルキー及び再生対象固有情報が X O R 演算処理され、その演算結果が復号化キーとされる。ステップ S 3 8 に示すように、いずれの条件にも一致されない場合には、ステップ S 4 0 において、再生対象ではないと判断され、復号処理が中断される。運用規則情報の再生対象制限フラグが 1 でなかった場合には、ステップ S 4 1 において、運用規則情報のタイトルキーがそのまま復号化キーとして復号化キー生成部 1 4 8 において設定される。復号化キーが設定されると、次に、ステップ S 4 2 に示すように暗号化されたコンテンツが読み込まれ、ステップ S 4 3 に示すように復号化キーを用いてコンテンツが復号化部 1 5 0 において復号化される。その後、ステップ S 4 4 において復号化されたコンテンツが書き出され、処理が終了される。

【 0 0 3 3 】

上述した実施例では、再生対象を限定する条件を、限定なし、端末に限定、個人に限定、端末と個人に限定、のいずれかの場合を前提に説明したが、限定条件はこれに限るものではなく、他の限定条件に換えられても、或いは、他の限定条件が付されても良いことは明らかである。

【 0 0 3 4 】

上述した実施例に係るコンテンツの暗号化方法及び暗号化されたコンテンツを復号化する復号化方法によれば、コンテンツが暗号化される際に、再生対象を限定するための固有情報は、再生対象固有情報として運用規則情報に組み込まれ、暗号化コンテンツと共に配信される。また、コンテンツが復号化される際には、

運用規則情報内の再生対象固有情報と、再生元の各種固有情報と比較することによって、再生条件を満たしているかどうかを確実に判断することが可能となり、コンテンツを復号化処理しなくても再生条件を判断することができる。従って、処理の効率化を図ることができる暗号化コンテンツを配信することができ、また、暗号化されたコンテンツの処理の効率化を図ることができる。

【 0 0 3 5 】

次に、この発明の他の実施例に係るコンテンツの暗号化方法及び暗号化されたコンテンツを復号化する復号化方法について図 6 から図 9 を参照して説明する。

【 0 0 3 6 】

図 6 は、この発明の他の実施例に係る暗号化処理の為の回路構成を機能ブロックで示すコンテンツ暗号化処理回路である。図 6 に示される機能ブロック回路は、実質的に図 1 に示す機能ブロック回路に同一であるので、図 1 と同一箇所には、同一符号を付してその説明を省略する。

【 0 0 3 7 】

図 6 に示されるコンテンツ暗号化処理回路では、運用規則情報生成部 1 1 2 に代えて暗号化されたキーワードを運用規則情報として生成する運用規則情報生成部 1 6 0 が設けられている。即ち、再生対象固有情報生成部 1 1 8 からの再生対象固有情報及びタイトルキー生成部 1 1 6 からのタイトルキーで暗号化キー生成部 1 1 4 で暗号化キーが生成され、また、再生対象固有情報を用いてキーワードが暗号化され、この暗号化キーワードがタイトルキーとともに運用規則情報生成部 1 6 0 で運用規則情報ファイルとして書き出される。

【 0 0 3 8 】

暗号化処理手順を示すフローチャートを示す図 7 を参照して図 6 に示したコンテンツ暗号化処理回路での暗号化処理について説明する。

【 0 0 3 9 】

図 7 に示されるコンテンツを暗号化する手順は、図 1 ～図 3 を参照して説明した第 1 実施例の暗号化処理とほぼ同一の手順で実行される。従って、図 4 において、図 1 に付した符号と同一の符号を付した処理は、同一の処理が実行されるものとしてその説明を省略する。

【 0 0 4 0 】

この他の実施例に係るコンテンツの暗号化方法においては、ステップ S 1 1 から S 2 3 が実行されて再生対象条件が限定されてタイトルキー及び再生対象固有情報から暗号化キーが生成された後に、第 1 の実施例と異なり、ステップ S 5 1 において、暗号化キー生成部 1 1 4 において、再生対象固有情報をキーとしてあらかじめ決められているキーワードが暗号化される。例えば、0 x 1 2 3 4 5 6 7 8 というキーワード値が再生対象固有情報をキーとして暗号化される。そして、以下同様にステップ S 2 7 ~ S 3 0 の処理が実行され、暗号化されたキーワードが運用規則情報生成部 1 6 0 に書き出され、この運用規則情報生成部 1 6 0 において、暗号化されたキーワード情報及びタイトルキーが運用規則情報ファイルとして書き出される。

【 0 0 4 1 】

図 8 には、暗号化処理で生成される運用規則情報のデータ構造が示されている。運用規則情報は、再生対象条件を限定するかどうかを示すフラグ 5 0 1 と、暗号化されたキーワード情報 5 0 2、タイトルキー 5 0 3 から構成される。再生対象を限定する場合には、再生対象限定フラグに 1 が設定され、このフラグ「1」によって、暗号化されたキーワード情報が有効であることが示される。逆に、再生対象を限定しない場合には、再生対象限定フラグに 0 が設定され、このフラグ「0」によって、暗号化されたキーワード情報が不定となる。暗号化処理で生成された暗号化データ及び運用規則情報は、サービスに応じてあらかじめ決められた方法で、再生端末へ配信される。

【 0 0 4 2 】

図 2 に示す再生端末では、図 9 に示すような手順に従い暗号化コンテンツが復号化処理される。図 9 に示される処理においては、図 5 に示したと同様の処理を含むことから、図 5 に付した符号と同一の符号を付した処理は、同一の処理が実行されるものとしてその説明を簡略にして説明する。

【 0 0 4 3 】

始めに、ステップ S 3 1 において、配信された運用規則情報が読み込まれる。次に、運用情報記憶部 1 4 4 に読み込まれた運用規則情報から再生対象限定フ

ラグが復号化キー生成部 1 4 8 で抽出され、ステップ S 3 2 において、再生対象限定フラグが 1 に設定されているかが判断される。フラグに 1 が設定されている場合、再生対象が限定されているものと判断され、ステップ S 3 3 において、復号化キー生成部 1 4 8 に端末固有情報が再生端末から入力され、ステップ S 3 4 において、個人固有項目情報が同様に入力される。

【 0 0 4 4 】

ここで、図 6 に示す処理においては、ステップ S 6 5 に示されるように、端末固有情報が再生対象固有情報として復号化キー生成部 1 4 8 においてにおいて設定される。次に、ステップ S 6 6 において、再生対象固有情報をキーにして、運用規則情報内の暗号化キーワード情報が復号化キー生成部 1 4 8 において復号化処理され、ステップ S 6 7 において、復号化されたキーワード情報があらかじめ決められたキーワード情報、例えば 0 x 1 2 3 4 5 6 7 8 と一致するかが判定される。両者が一致しない場合には、ステップ S 6 8 において、個人固有項目情報が再生対象固有情報として設定される。次に、ステップ S 6 9 において、再生対象固有情報をキーにして、復号化キー生成部 1 4 8 において、運用規則情報内の暗号化キーワード情報が復号化処理され、ステップ S 7 0 において、復号化されたキーワード情報があらかじめ決められたキーワード情報と一致するかが判定される。両者が一致しない場合、ステップ S 7 1 において、端末固有情報と個人固有項目情報から再生対象固有情報が復号化キー生成部 1 4 8 において生成される。例えば、端末固有情報及び個人固有項目情報が X O R 演算処理されて求められた演算結果が再生対象固有情報に定められる。ステップ S 7 2 において、再生対象固有情報をキーにして、運用規則情報内の暗号化キーワード情報が復号化キー生成部 1 4 8 において復号化処理され、ステップ S 7 3 において、復号化されたキーワード情報があらかじめ決められたキーワード情報と一致するかが判定される。

【 0 0 4 5 】

上記ステップ S 6 7、S 7 0、S 7 3 において、いずれかの条件にて、暗号化キーワードからキーワードが復号されている場合には、再生対象であると判断され、ステップ S 3 9 において、運用規則情報内のタイトルキーと再生対象固有情

報から復号化キーが生成される。例えば、タイトルキー及び再生対象固有情報の XOR 演算処理した演算結果が復号化キーとされる。ステップ S 6 7、S 7 0、S 7 3 において、いずれの条件にも一致しなかった場合には、復号化キー生成部 1 4 8 において再生対象ではないと判断され、ステップ S 4 0 において、復号処理が中断される。ステップ S 3 2 において、運用規則情報の再生対象制限フラグが 1 でなかった場合には、ステップ S 4 1 において、運用規則情報のタイトルキーがそのまま復号化キーとして設定される。ステップ S 4 1 或いは S 3 9 において、復号化キーが設定されると、ステップ S 4 2 において、暗号化されたコンテンツが復号化部 1 5 0 に読み込まれ、ステップ S 4 3 において、復号化キーを用いてコンテンツが復号化される。その後、ステップ S 4 4 において、復号化されたコンテンツが書き出されて処理が終了される。

【 0 0 4 6 】

この他の実施例では、再生対象を限定する条件を、限定なし、端末に限定、個人に限定、端末と個人に限定、のいずれかの場合を前提に説明したが、限定条件はこれに限るものではなく、他の限定条件に換えられても、或いは、他の限定条件が付されても良いことは明らかである。

【 0 0 4 7 】

以上、図 6 から図 9 に示された他の実施例によれば、コンテンツが暗号化される際に、再生対象を限定するための固有情報をキーにキーワードが暗号化され運用規則情報に組み込まれ、暗号化コンテンツと共に配信される。また、コンテンツが復号化される際には、再生元の各種固有情報をキーに運用規則情報内の暗号化キーワードを正しく復号化できるかどうかを判断することで、再生条件を満たしているかどうかを確実に判定することができる。従って、処理の効率化を図ることができる暗号化コンテンツを配信することができ、また、暗号化されたコンテンツの処理の効率化を図ることができる。

【 0 0 4 8 】

【発明の効果】

以上のように、コンテンツの再生対象を限定した場合においても、コンテンツを再生する際に、再生条件を満たしているかどうかを、コンテンツを復号化し

なくとも確実に判断できる暗号化方法及び暗号化されたコンテンツを復号化する復号化方法が提供される。

【図面の簡単な説明】

【図 1】

この発明の一実施例に係るコンテンツの暗号化方法を実現するための機能ブロックを示す説明図である。

【図 2】

この発明の一実施例に係る暗号化されたコンテンツを復号化する復号化方法を実現するための機能ブロックを示す説明図である。

【図 3】

この発明の一実施例に係るコンテンツの暗号化方法を示すフローチャートである。

【図 4】

図 3 に示された方法によって作成される運用規則情報ファイルのフォーマットを示す平面図である。

【図 5】

この発明の他の実施例に係る暗号化されたコンテンツの復号化方法を示すフローチャートである。

【図 6】

この発明の他の実施例に係るコンテンツの暗号化方法を実現するための機能ブロックを示す説明図である。

【図 7】

この発明の他の実施例に係るコンテンツの暗号化方法を示すフローチャートである。

【図 8】

図 7 に示された方法によって作成される運用規則情報ファイルのフォーマットを示す平面図である。

【図 9】

この発明の他の実施例に係る暗号化されたコンテンツの復号化方法を示すフ

ローチャートである。

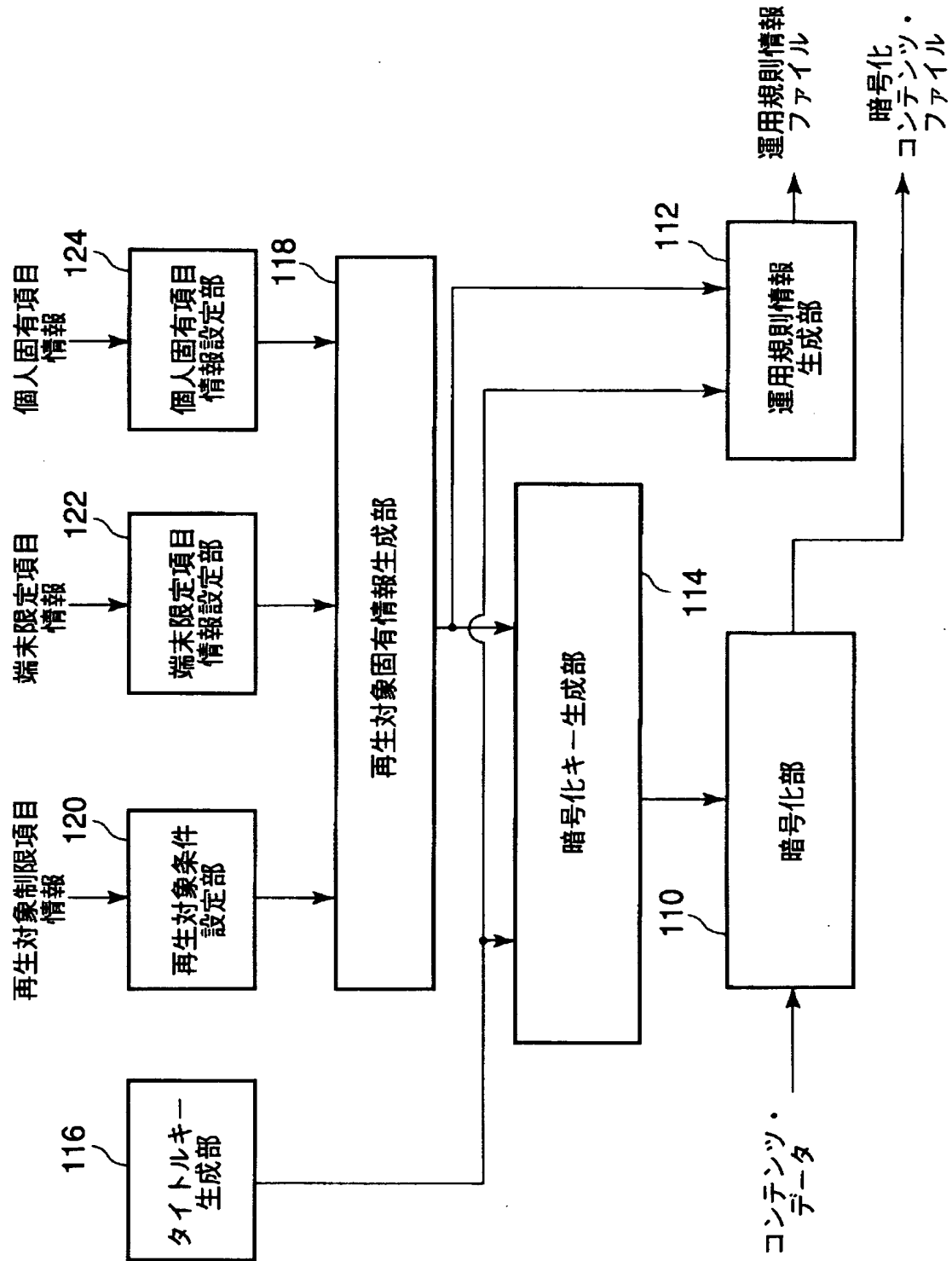
【符号の説明】

- 1 1 0 . . . 暗号化部
- 1 1 2、1 6 0 . . . 運用規則情報生成部
- 1 1 4 . . . 暗号化キー生成部
- 1 1 6 . . . タイトルキー生成部
- 1 1 8 . . . 再生対象固有情報生成部
- 1 2 0 . . . 再生対象条件設定部
- 1 2 4 . . . 個人固有項目情報設定部
- 1 4 2 . . . ファイル受信部
- 1 4 4 . . . 運用情報記憶部
- 1 4 6 . . . 暗号化コンテンツ・データ記憶部
- 1 4 8 . . . 復号化キー生成部
- 1 5 0 . . . 復号化部

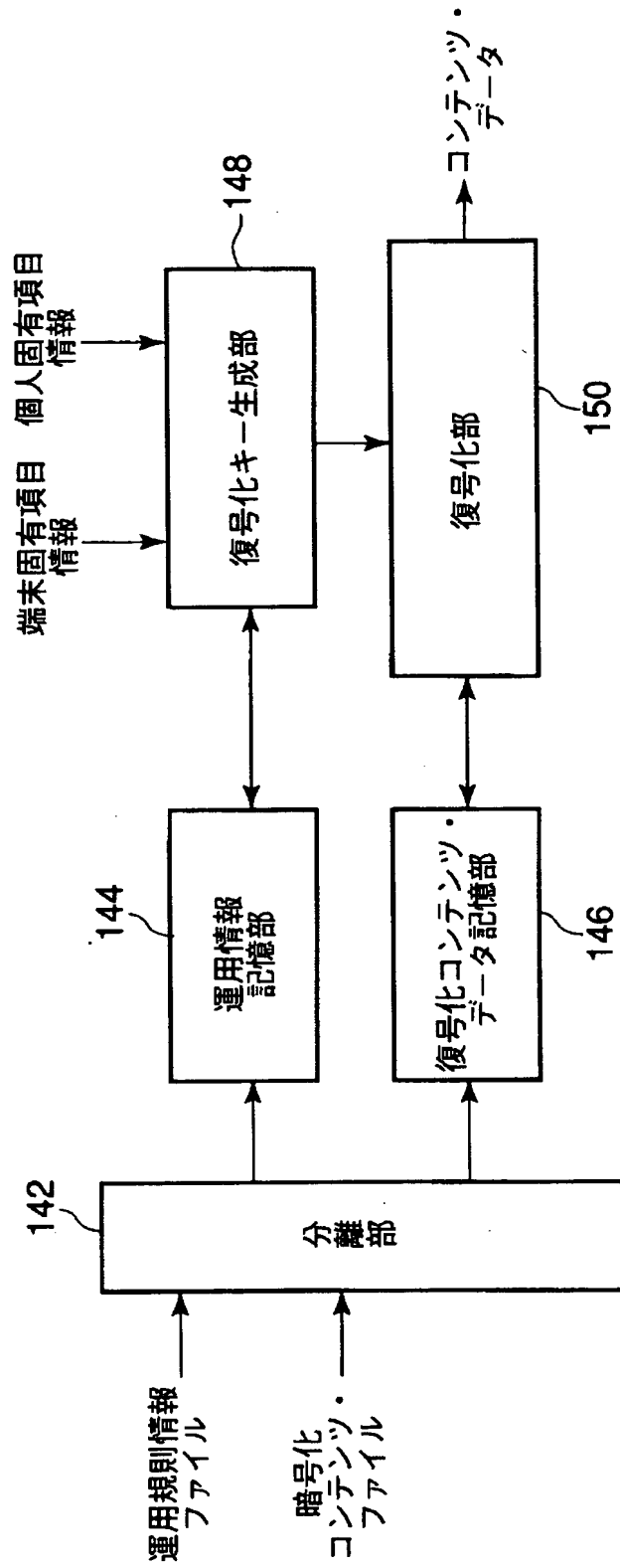
【書類名】

図面

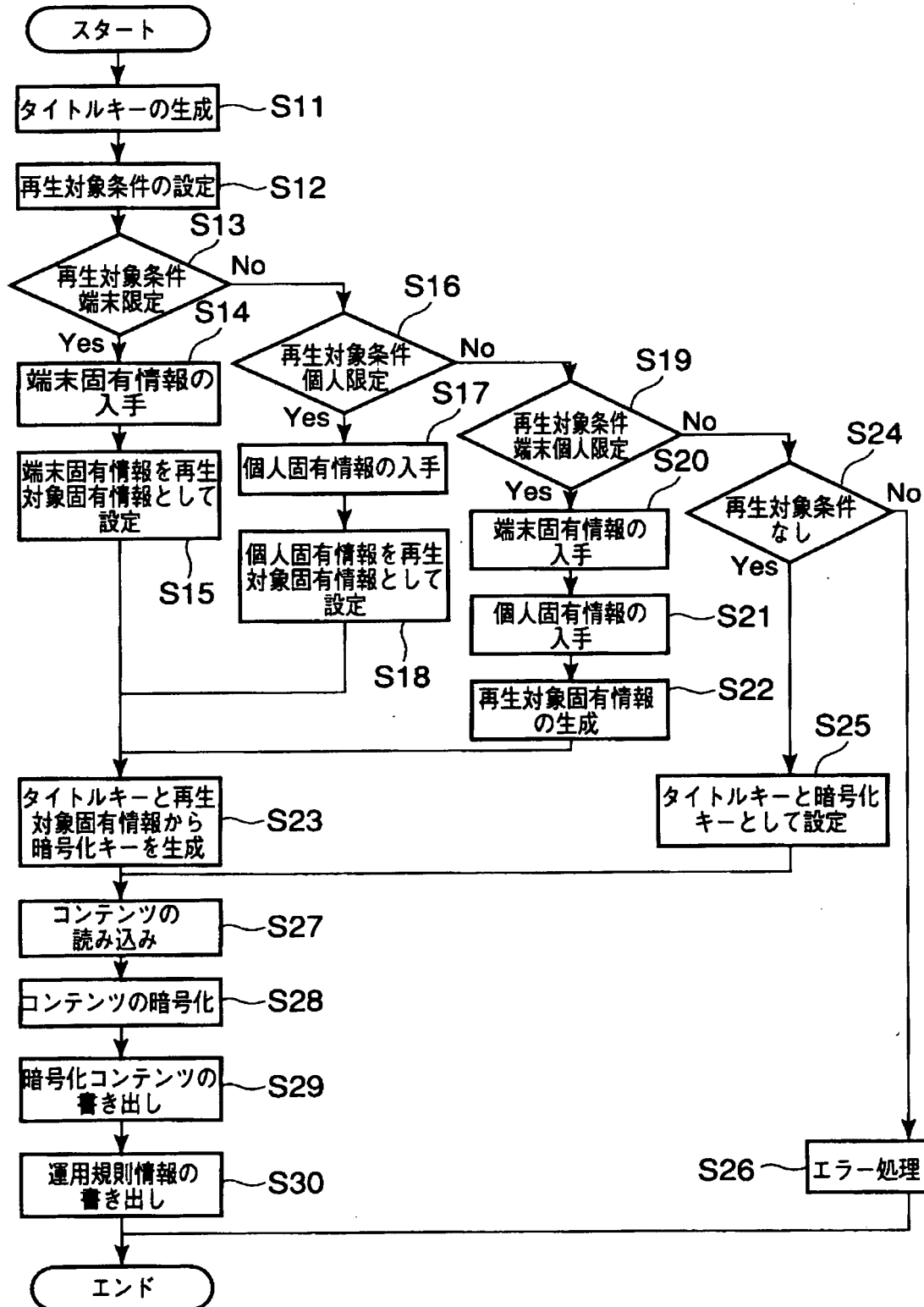
【図 1】



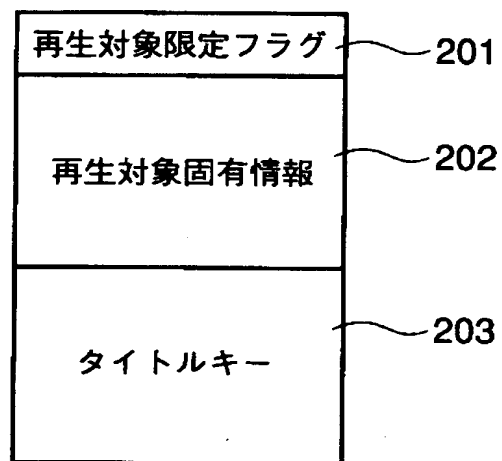
【図 2】



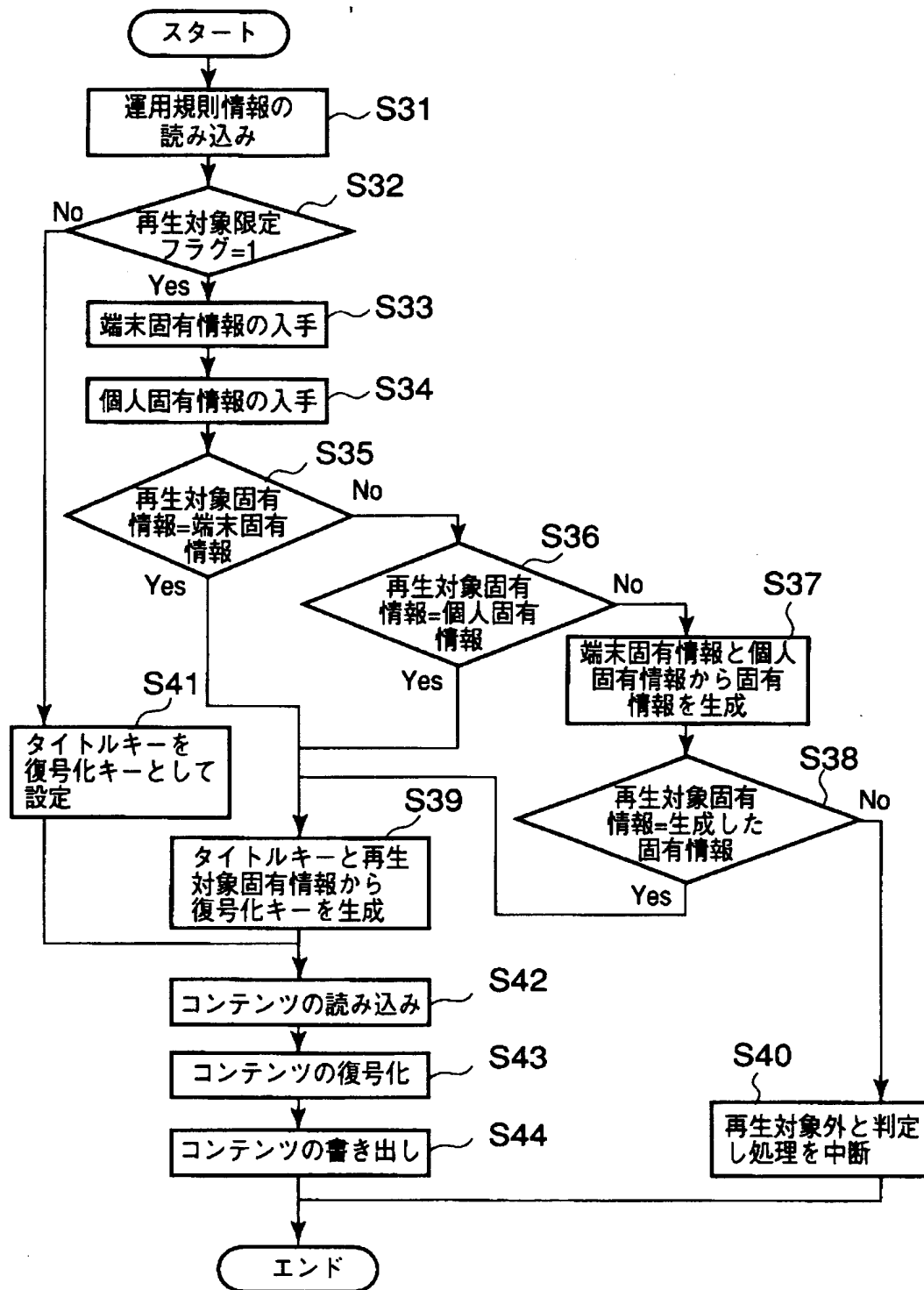
【図 3】



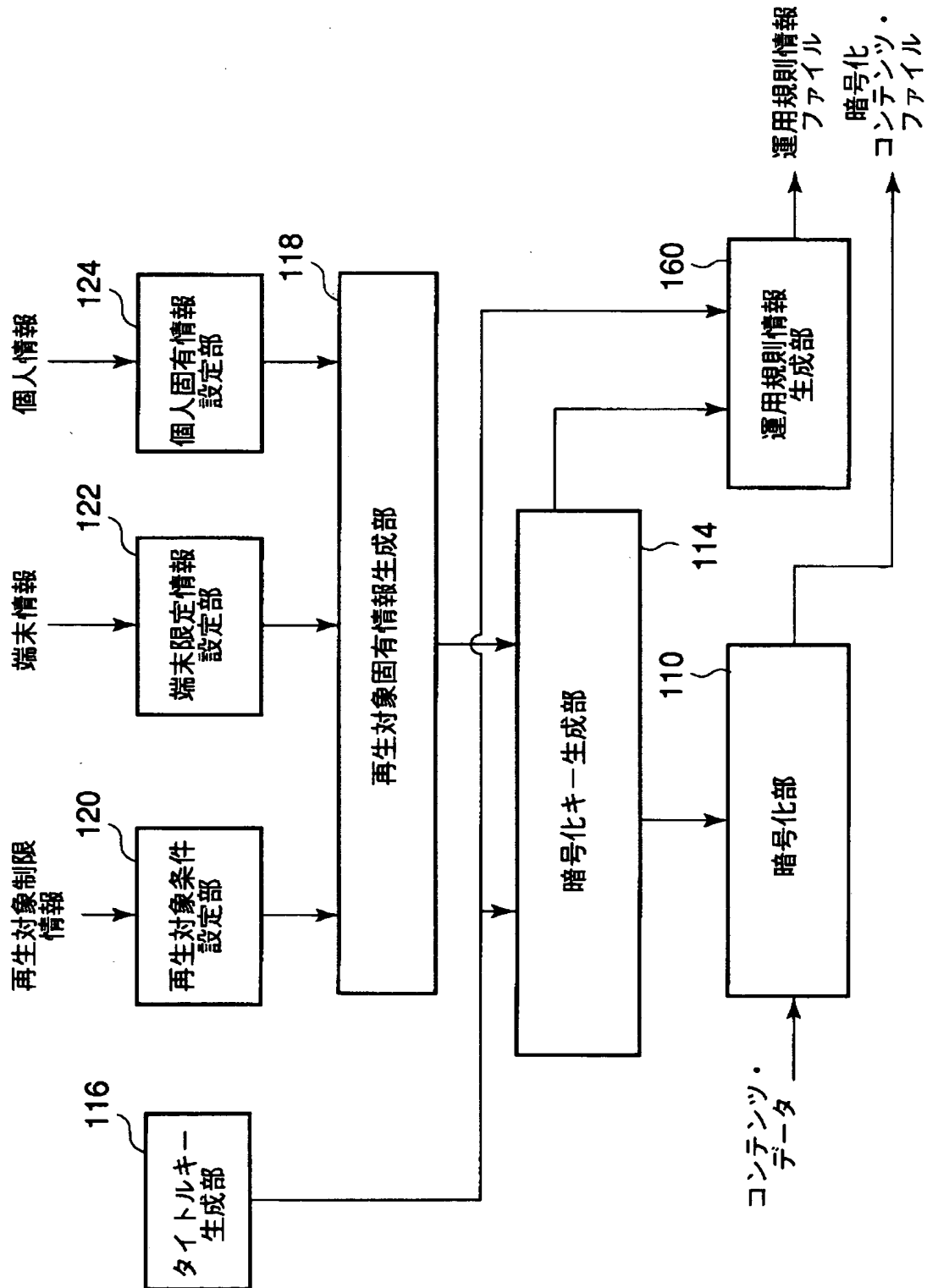
【図 4】



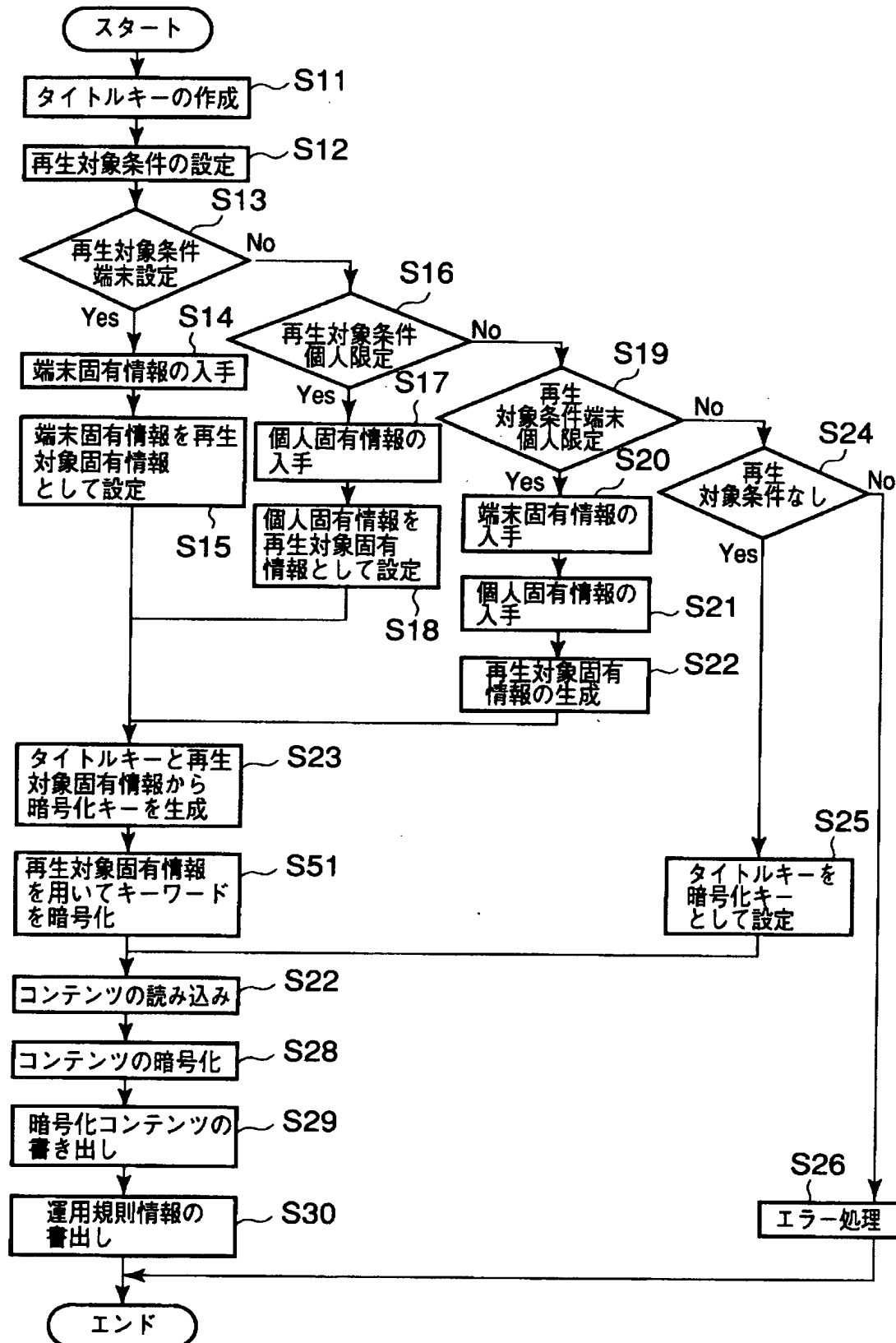
【図 5】



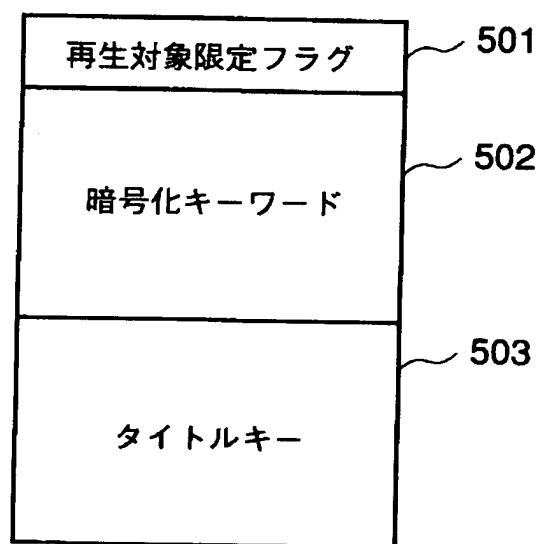
【図6】



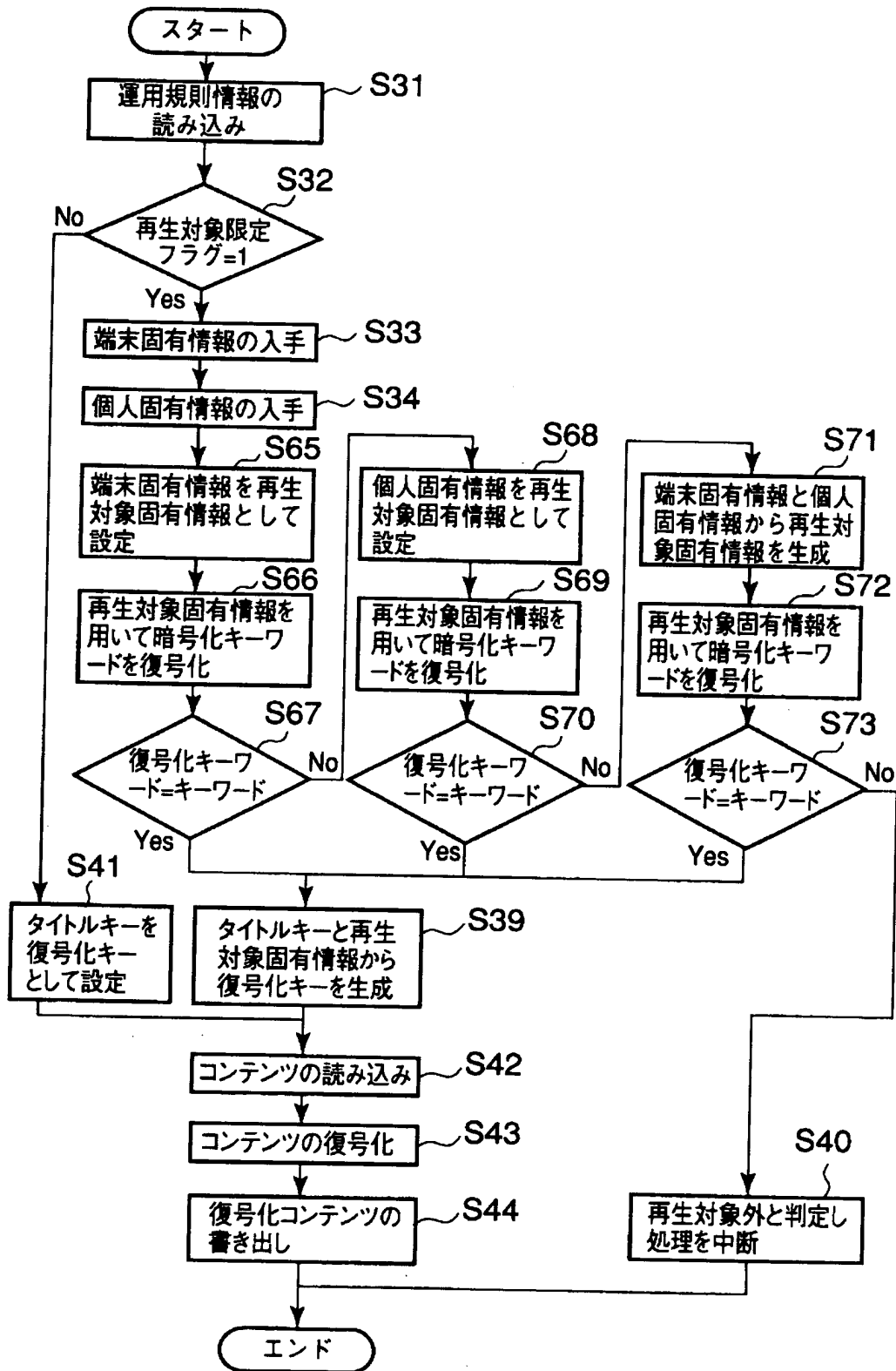
【図 7】



【図 8】



【図 9】



【書類名】 要約書

【要約】

【課題】 コンテンツの再生に際して再生条件を満たしているかどうかを、コンテンツを復号化なしに判断できる復号化方法を提供するにある。

【解決手段】 暗号化データを復号化する方法においては、コンテンツ毎にユニークに決まるタイトルキーと端末を限定する項目情報を含みコンテンツの再生対象を限定する固有情報とが組み合わされた運用規則情報及び前記タイトルキーと前記固有情報から生成される暗号化キー情報とを基に暗号化されている暗号化コンテンツ・データを受け取り、端末側装置から項目情報が取得され、この項目情報と前記運用規則情報とから暗号化コンテンツ・データの再生可能性が判定される。この判定に従って、前記項目情報及びタイトルキーから復号化キーが生成され、コンテンツ・データは、この復号化キー情報を基に復号化される。

【選択図】 図 2

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日	2001年 7月 2日
[変更理由]	住所変更
住 所	東京都港区芝浦一丁目1番1号
氏 名	株式会社東芝